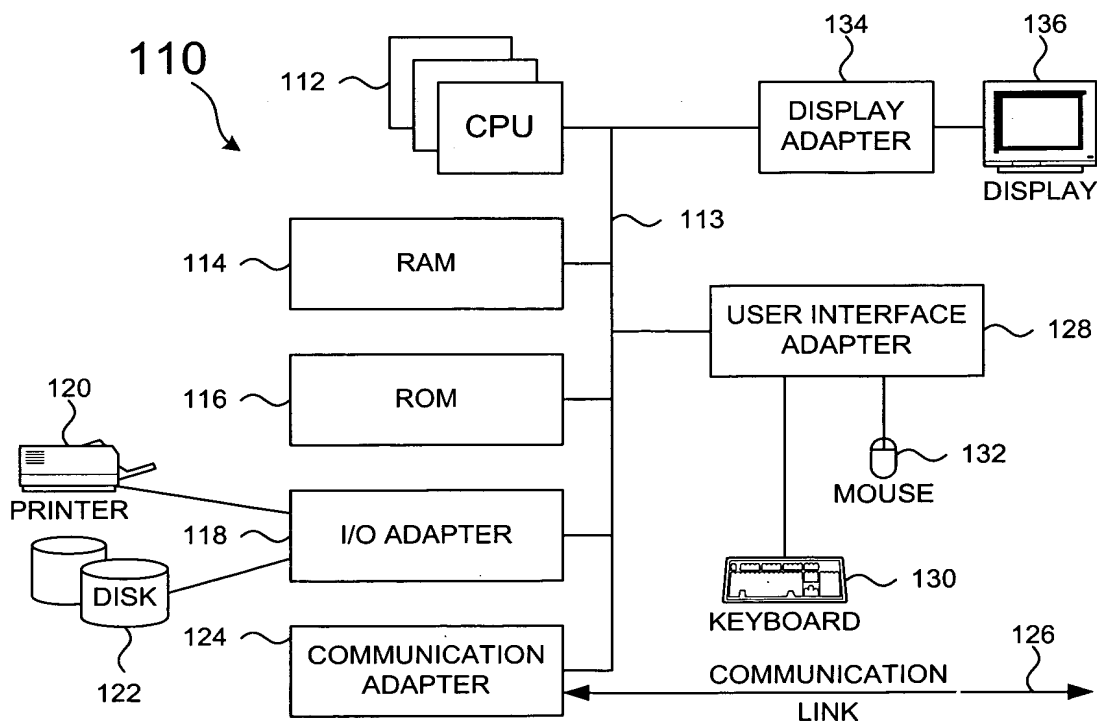
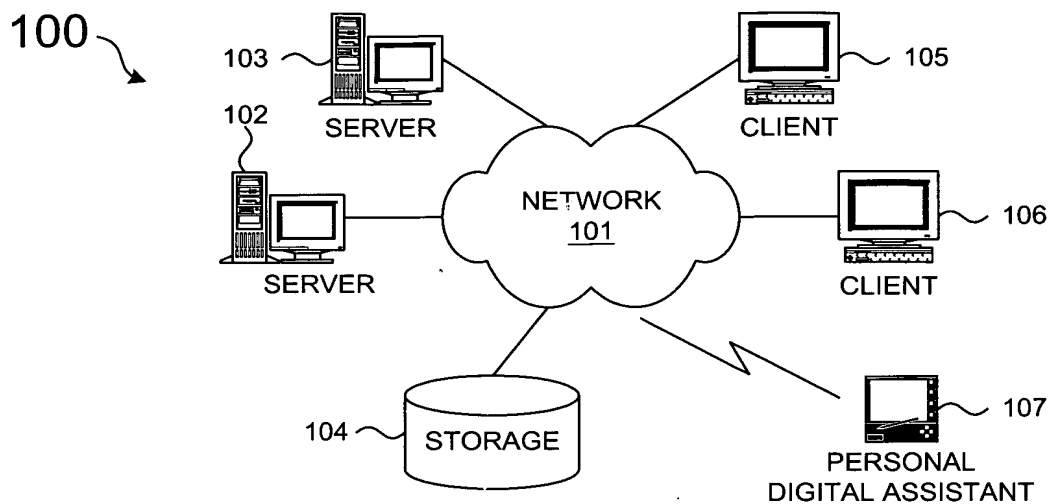


1/7



2/7

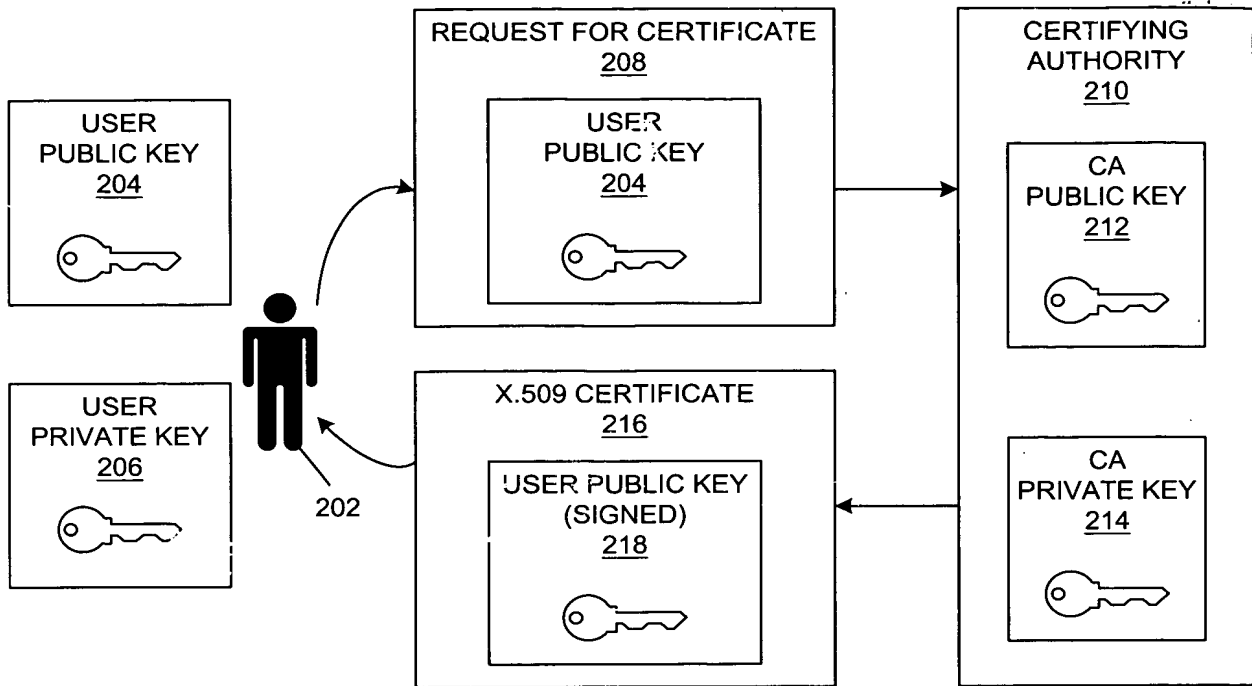


FIG. 2
(PRIOR ART)

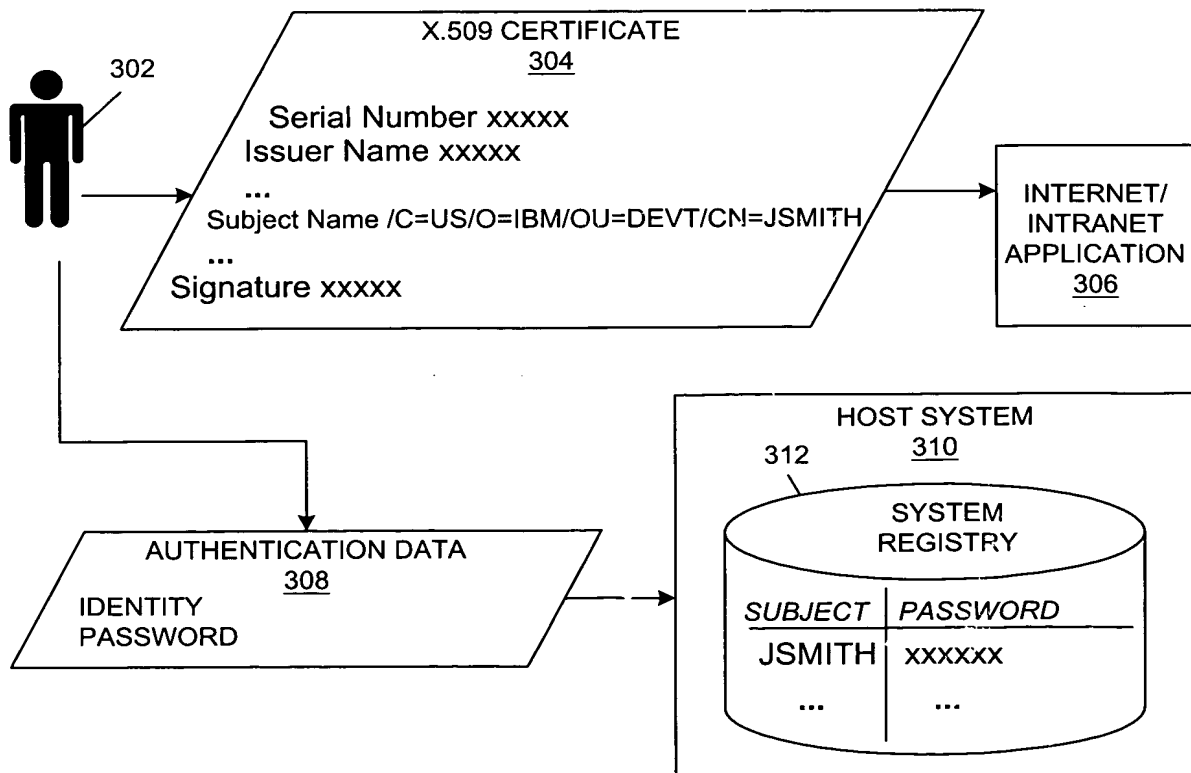


FIG. 3

3/7

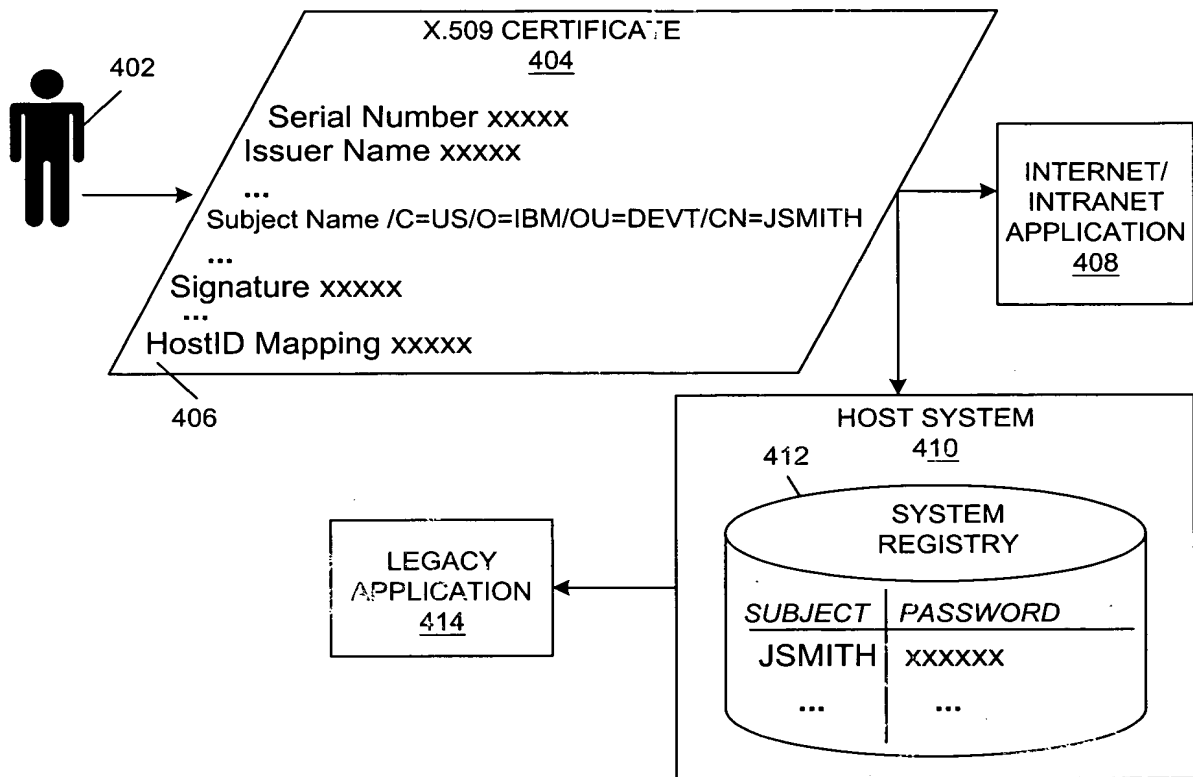


FIG. 4

```

HostIdMapping ::= SEQUENCE {
    hostName          [1] IMPLICIT IA5String,
    subjectID         IMPLICIT IA5String,
    proofOfIdPossession IdProof OPTIONAL }

IdProof ::= SEQUENCE {
    secret            OCTET STRING,
    encryptionAlgorithm OBJECT IDENTIFIER }
    
```

FIG. 6

4/7

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm  AlgorithmIdentifier,
    signature            BIT STRING }

TBSCertificate ::= SEQUENCE {
    version             [0] Version DEFAULT v1,
    serialNumber        CertificateSerialNumber,
    signature            AlgorithmIdentifier,
    issuer              Name,
    validity             Validity,
    subject              Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID       [1] IMPLICIT UniqueIdentifier OPTIONAL,
    subjectUniqueID      [2] IMPLICIT UniqueIdentifier OPTIONAL,
    extensions           [3] Extensions OPTIONAL }

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
    notBefore           Time,
    notAfter            Time }

Time ::= CHOICE {
    utcTime              UTCTime,
    generalTime          GeneralizedTime }

UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm            AlgorithmIdentifier,
    subjectPublicKey     BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
    extnID               OBJECT IDENTIFIER,
    critical              BOOLEAN DEFAULT FALSE,
    extnValue             OCTET STRING }
```

FIG. 5
(PRIOR ART)

5/7

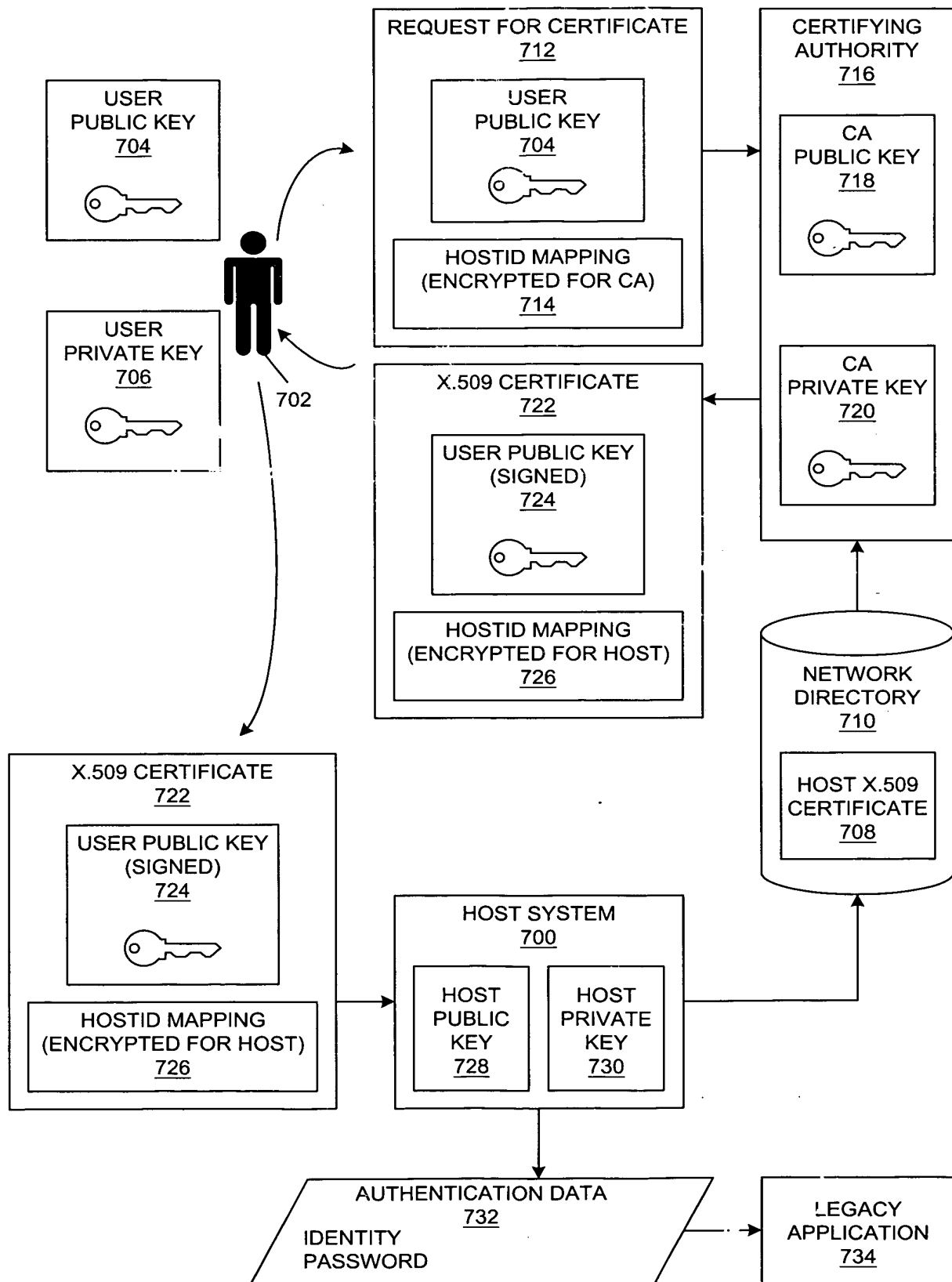


FIG. 7

6/7

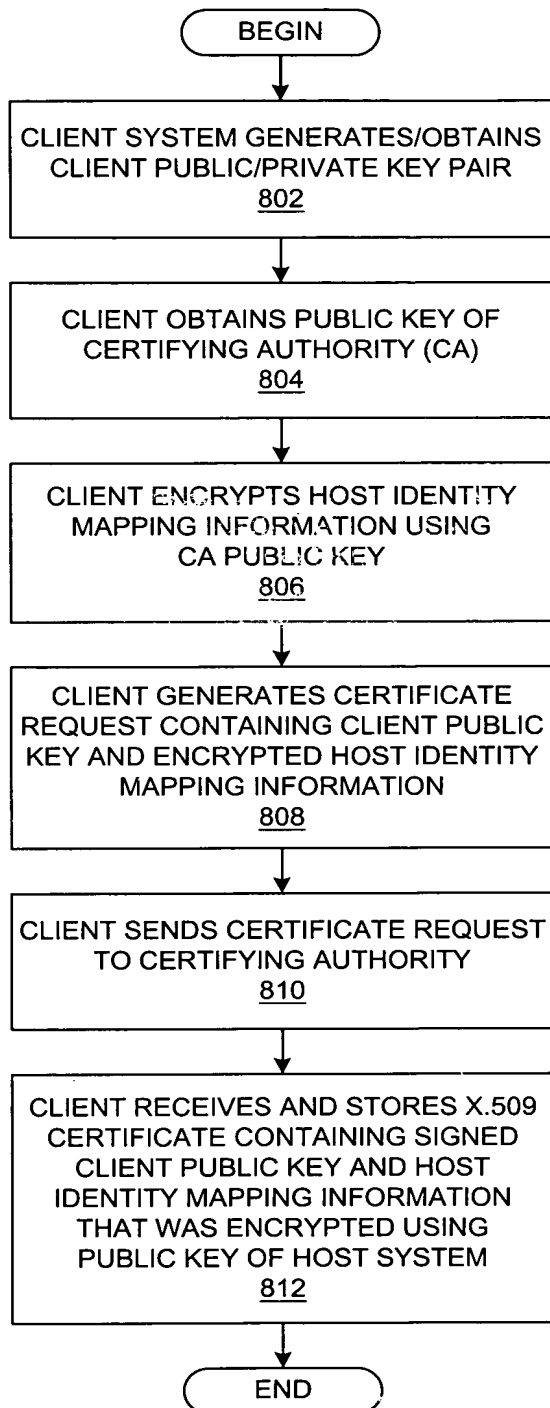


FIG. 8A

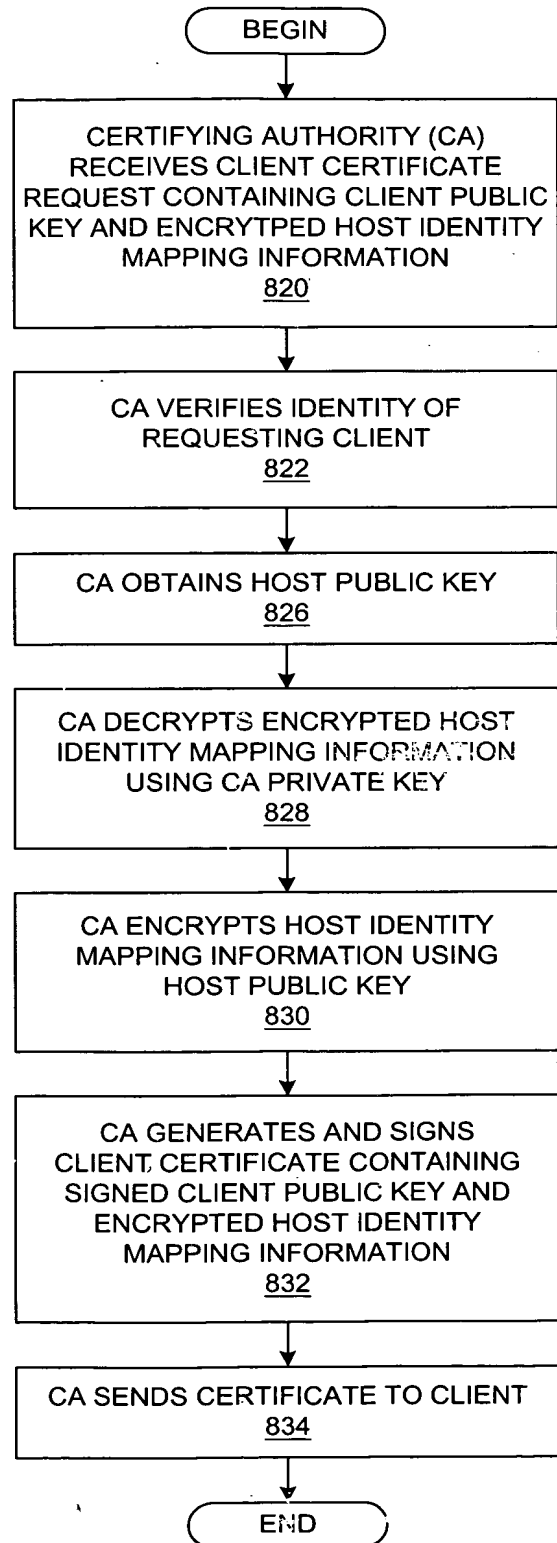


FIG. 8B

7/7

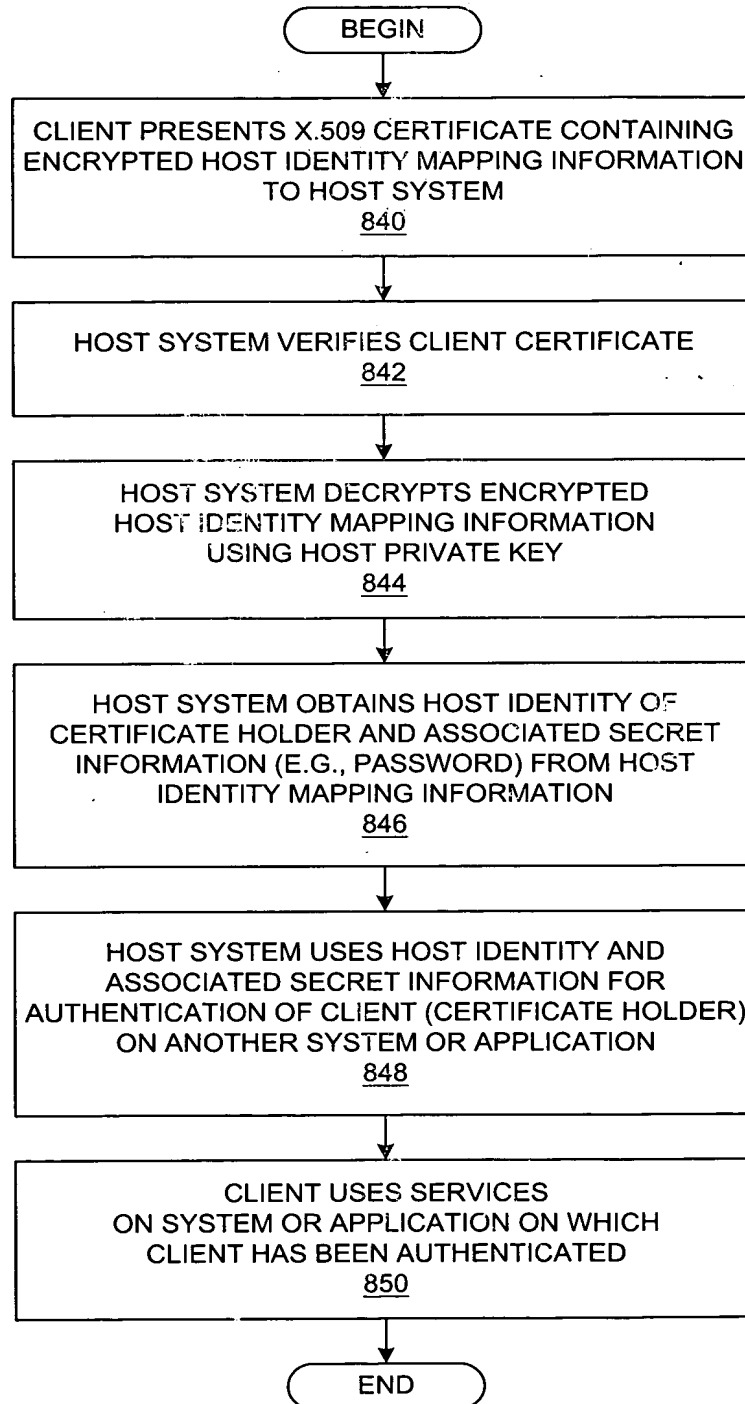


FIG. 8C